2017年信息科学热点回眸

万赟

美国休斯敦大学维多利亚分校,德克萨斯州维多利亚 77901

摘要　回顾2017年信息科学的热点:加强学习算法在人工智能领域的应用取得显著效果,量子计算机的竞争已经进入到50量子比特阶段,智能家庭进一步大众化,机器人仿真技术更加成熟。同时2017年信息科学领域也出现了很多挑战,例如:人工智能算法不可避免地受到历史数据所暗藏的人类偏见的影响,互联网假新闻影响到了美国大选,比特币呈现泡沫化升值,威胁计算机用户的勒索病毒也愈演愈烈。

关键词　人工智能;量子计算机;比特币;勒索病毒

2017年信息技术领域的重大突破仍然以人工智能的应用为主。其中研发出AlphaGo的DeepMind公司通过加强学习算法继续在人工智能棋类领域独领风骚。IBM,谷歌等公司在量子计算机的实用化方面也取得了重要的进步。机器人仿真技术飞速发展,在自然语言沟通和动作模拟方面产生了飞越性发展。另一方面,人工智能的发展也不可避免地带来了一些负面的影响,例如人类社会的种种偏见被人工智能通过数据挖掘而捕捉,并成为一种新规则,影响到人们生活的方方面面;社交媒体成为假新闻的传播渠道。另外,比特币在2017年一路飙升到接近2万美元,成为人类历史近500年来最大的经济泡沫,与之相关的网络勒索病毒在2017年的流行也成为人们的新挑战。

1　加强学习算法效果显著

被谷歌收购的DeepMind公司在2017年利用加强学习(reinforcement learning)方式接连成功培训出新一代人工智能围棋程序AlphaGo Zero和AlphaZero,前者成功击败AlphaGo,后者则不仅击败了AlphaGo,还通过短时间学习成功击败了当前实力最强的国际象棋和日本将棋人工智能程序。所谓加强学习算法就是让程序从随机状态开始,通过自我对弈来提高能力。每一次落子前,程序计算出不同位置的胜率,挑选出胜率最大的位置,事后根据实际的结果调整计算胜率的神经网络权重。DeepMind公司的团队在培训AlphaGo Zero时采用了机器自我培训的方式。而之前训练AlphaGo时使用的是人类过去的棋谱对局,相当于人来培训机器。这两种方式在效率和效果上存在巨大差距——训练AlphaGo Zero时使用的是配备4个高性能处理器(TPU)的单机,耗时3天,总计490万场对局,而训练AlphaGo时使用了多台计算机,共48个TPU,耗时数月,总计3000万场对局(图1)。结果AlphaGo Zero在与AlphaGo进行的100场对弈中获得全胜。这一成果发表在2017年10月19日《Nature》杂志上[1]。

接下来DeepMind团队把加强学习的方式进一步简化,结合深度学习神经网络,推出了普适性更强的AlphaZero人工智能程序。该程序在初始状态时只需要输

收稿日期:2017-12-25;修回日期:2018-01-05

作者简介:万赟,教授,研究方向为互联网与电子商务,电子信箱:yunwan@gmail.com

引用格式:万赟. 2017年信息科学热点回眸[J]. 科技导报, 2018, 36(1): 91-97; doi: 10.3981/j.issn.1000-7857.2018.01.010

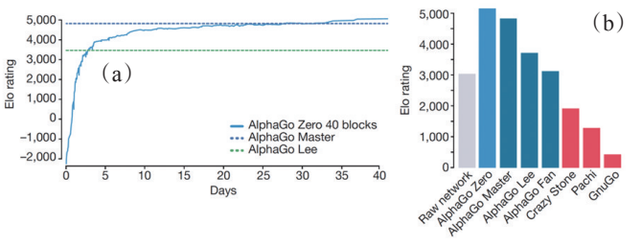

图1 AlphaGo Zero与其他算法的训练时间与效果比较[1]

某种棋类的基本规则,无需其他知识,然后从零开始自学训练。结果AlphaZero仅用4 h自学击败了目前最强的国际象棋人工智能程序Stockfish(28赢,72平),2 h自学击败了最强的日本将棋(Shogi)人工智能程序Elmo,8 h自学击败了AlphaGo,34 h自学击败了前面提到的训练了3天的AlphaGo Zero(图2)。值得一提的是,Stockfish使用的计算机每秒可以计算7000万个棋子位置,而AlphoZero使用的计算机只能计算8万个位置,这相当于前者比后者可以多考虑未来8步棋的走势,但AlphaZero仍然获得了胜利,这是因为AlphaZero使用了更类似人脑思维方式的深度学习神经网络来权衡每一步的利弊,这一优势弥补了计算能力方面的不足。这一成果有可能改写人工智能搜索领域的很多共识,例如传统认为计算机擅长的全面遍历各种可能性的Alpha-beta剪枝算法在搜索最优步骤方面具有先天优势,但是AlphaZero的成功意味着人类棋手通过对所谓全局"势"的判断来决定下一步走法的这种高度过滤性思考方式其实具有更大的优势。2017年12月5日,该成果刊登在康奈尔大学的开源论文网站arXiv上[2]。

加强学习算法的成功应用意味着在不远的将来可以用这一方式解决很多具有类似思考模式的问题,例如医疗诊断、故障分析等。

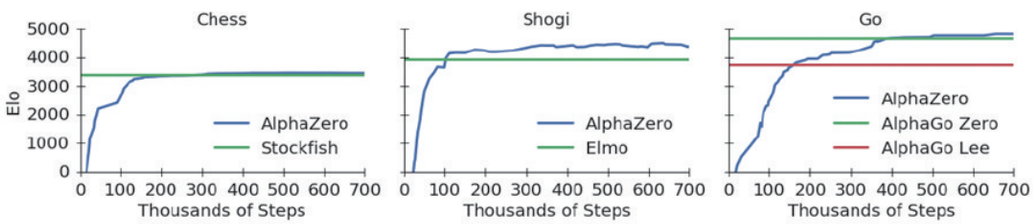

图2 AlphaZero与其他算法的计算效率对比[2]

2 量子霸权逐见分晓

量子计算机是目前仅次于人工智能的研究热点。2017年量子计算机技术进一步走向成熟。目前国际上量子计算机竞争的主要参与者包括IBM、谷歌、英特尔、微软,以及中国科学院。英特尔专注硅量子点技术,微软选择拓扑量子计算,两者都比较冷门,IBM 和谷歌选择的则都是比较主流的超导回路技术——回路在低温超导状态下电流的2个方向分别代表0和1。因而世界量子计算机的竞争主要在IBM和谷歌之间展开。

量子计算机的每个量子比特在任意时刻可以同时包含0和1两个位元状态,而传统计算机的一个位元在任意时刻只能包含一种信息状态(0或1)。当量子计算机的量子比特数位增加时,它任意时刻包含的信息量可以呈指数增长,例如具有10个量子比特的量子计算机可以同时包含1024个不同数字,而10位元的传统计算机只能包含这1024个不同数字中的一个。这一特点意味着49个量子比特就可以表示1亿亿(10^{16})个不同数字,而传统计算机只有配备拍字节(petabyte)的内存才可能储存同样多的数字。目前世界上最大的计算机内存是惠普在2017年5月份推出一台计算机原型上配备的160 TB内存,也只有其16%(1 PB相当于1000 TB)。所以谁先设计出第一台能够稳定使用49量子比特的量子计算机就意味着在计算领域取得了"传统超级计算机所不具有的能力"[3],也就是量子霸权(quantum supremacy)。

2017年5月,中国科技大学潘建伟团队在上海宣布成功构建10量子比特量子计算机。2017年4月谷歌宣布要在2017年底打造出世界上第一台可以超越传统计算机的量子计算机,实现49个量子比特的操纵,10月验证成功了利用超导回路搭建49量子比特计算机的可行性。 IBM的进步似乎更为神速,2017年3月IBM对外宣布将在年内推出全球第1个20量子比特的商业化量子计算云服务——IBM Q,这是世界上第1个收费的量子计算云服务系统;11月宣布研制成功50量子比特的量子计算机原型(图3);其量子计算机的量子态保持时

间均达到了90 μs,刷新了业界的记录。

由于量子计算机需要全新的软件和编程平台,这方面的竞争也已经开始。微软公司在2017年12月正式推出了测试版量子计算编程语言Q#。IBM则在早些时候开发出QISKit量子信息软件处理工具包,可最大限度利用量子计算系统的核心。

在量子通信领域,2017年8月10日,全球首颗量子科学实验卫星"墨子号"圆满完成了三大科学实验任务:量子纠缠分发、量子密钥分发、量子隐形传态。使得中国在量子通信领域达到新高度[4]。

图3　IBM 50量子比特计算机

3　智能家庭进一步发展

2017年人工智能技术以不同方式继续进入并影响到人类社会多个领域。谷歌和亚马逊在智能家庭领域展开全面竞争。亚马逊Echo最早在2015年进入家庭智能领域,2016年推出用于卧室的Echo Dot,2017年连续推出了用于拍摄衣着和推荐时装的Echo Look,用于播放视频、拨打视频电话的Echo Show和Echo Spot,以及Echo升级后的家庭智能核心Echo Plus。这一系列产品的推出进一步奠定了亚马逊在智能家庭领域的领先地位。

谷歌在这一领域的实力也在2017年有了长足的发展。谷歌Home(图4)在2016年11月首次进入市场,虽比亚马逊晚一年,但2017年谷歌连续推出了Home Mini和Home Max两种新成员,给用户更多的选择。其中Home Max引入了智能声音技术,通过人工智能感知周围环境的变化,并根据变化自动调节音量。

苹果公司原计划在2017年12月推出主打的智能家庭硬件核心HomePod,但是最终没能及时完善一些技术细节,不得不推迟发布,错失了圣诞节销售时机。

智能家庭硬件和软件的大量普及将在未来几年全面升级,并改变很多家庭获取信息和安排各种生活细节的传统习惯和方式。其中最显著的一点是随着计算机智能化的提高,普通大众的人机交互方式将从键盘沟通逐渐全面转变为自然语言沟通。

另一方面,智能家庭的数据传输涉及很多个人信息,所以如何保护私密信息不被泄露成为日益重要的研究方向。研究显示,即使在加密情况下,目前流行的智能家庭核心部件均存在不同程度的数据泄露问题[5]。

图4　谷歌Home和亚马逊Echo系列

4　机器人仿真更加成熟

机器人仿真领域在2017年取得稳步进展。这一领域备受关注的公司之一是2013年被谷歌收购的波士顿动力公司(Boston Dynamics)。该公司脱胎于麻省理工学院的研究项目,并通过美国国防高等研究计划署(DARPA)资助研制出高度仿真的波士顿机械狗而著称于世。2017年,该公司研制的ATLAS仿真机器人成功实现了后空翻高难度动作(图5)[6],再次受到业界和大众的瞩目。

图5　ATLAS的高难度后空翻动作

收购波士顿动力公司是谷歌公司Android操作系统的创始人安迪·鲁宾(Andy Rubin)做出的决定。随着2014年鲁宾的离去,谷歌在机器人领域的进取动力迅速下降。2017年6月,波士顿动力公司被日本软银集团收购,谷歌公司暂时离开了机器人仿真领域。日本在机器人仿真领域一直占据领先地位,软银集团对波士顿动力公司的收购将进一步巩固日本公司在这一领域的地位。

2017年10月11日,联合国副秘书长阿米娜·穆罕默德在议题为"一切的未来——快速技术变革的时代的可持续发展"的联合国大会第二委员会和经济及社会理事会联合会议上采访了由香港汉森机器人技术公司(Hanson Robotics)研制的社交机器人索菲亚(Sophia,图6)。汉森公司以开发模拟真人的机器人著称。索菲亚在外型上和2015年科幻片《机械姬》里面的女机器人主人公非常相似。不仅如此,索菲亚能够与人进行流利的自然语言沟通,拥有自己的推特账户(@SophiaTheRobot2)。沙特阿拉伯甚至授予了索菲亚公民权,使它成为地球上第1个机器人公民。

图6 索菲亚与联合国副秘书长阿米娜·穆罕默德讨论未来可持续性发展(图片来源:http://www.un.org/apps/news/story.asp?newsid=57860#.Wk75lVQ-fBI)

5 克服算法偏见成为共识

将机器人与网络联通,让其不断学习来自网络的信息,并通过与人沟通来提高语言能力是最近两年不少公司和研究机构的研发方向,但是从反馈来看,这一方式很容易受到人类业已存在的歧视和偏见的影响。2010年谷歌的相片标签算法把用户上传的家庭照片里的黑人标注为大猩猩,引起很多人的不满,不得不公开道歉。2016年,微软公司将聊天机器人Tay连入Twitter,试图通过Twitter用户与其沟通来学习人类的各种知识和习惯,但仅仅24 h后就不得不将其下线。因为Twitter用户不断对其灌输各种种族偏见和歧视论点,将Tay很快"培养"成一个不断表达种族偏见和各种歧视观点的机器人[7]。2017年,英国一家医学院发现其招生程序的人工智能算法将女性和少数民族申请人的录取概率自动降低,原来该算法是将以前的招生录取数据进行数据挖掘生成的,所以"继承"了以往以白人男性为主的招生录取人员的个人偏见。

类似的事件还有很多,美国佛罗里达某警局使用的再犯罪预测程序的错误预测案例中,黑人被预测再犯罪的概率高于白人2倍。谷歌翻译算法在职业相关的翻译中,自动将土耳其语中性别中立的人称代词翻译为"他是医生"和"她是护士"。一款尼康相机在引入人工智能识别算法后,每当亚洲用户拍摄家庭照片时,会自动提示是否照片中有人眯眼。这些现象都指向了一个问题,就是在人们不断引入人工智能技术的同时,传统的偏见也伴随培训人工智能技术的数据被引入到预测结果中[8]。

针对这一现象,普林斯顿和巴斯大学的学者最近在《Science》上发表《Talking to bots: Sgmbiotic gency and the case of tay》(图7)[9]通过对大量自然语言文本关联分析,发现在这些人工智能算法普遍使用的文本里,语言的关联准确地刻画了人类的各种历史偏见,其中

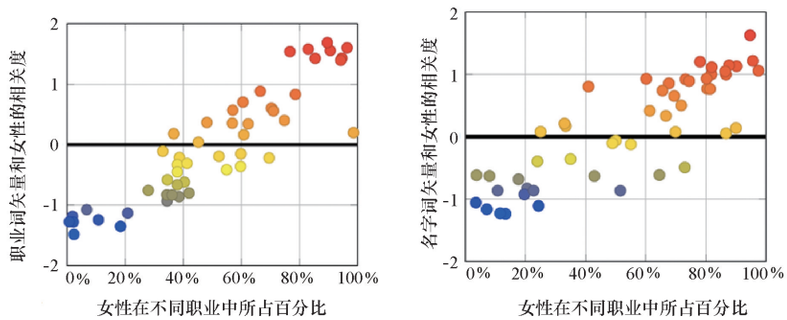

图7 该研究发现职业和女性以及名字和女性呈现非常类似的高度相关性[9]

不仅包括道德中立的对自然物种的偏见,还包括对种族、性别、职业,甚至是个人姓名的偏见。这一发现虽然还不足以立即消除偏见,却为将来克服这一问题提供了比较清晰的思路[9]。

6　假新闻肆虐互联网

美国纽约大学和斯坦福大学的研究人员通过对网络浏览数据、网络事实调查网站数据和网上民调数据分析,发现有14%的美国大众将社交媒体列为重要的选举新闻信息来源。在2016年大选前3个月里支持唐纳德·特朗普的选民一共分享了3000万次来自Facebook的假新闻,支持希拉里·克林顿的选民只分享了800万条假新闻。1位普通的美国民众在大选前几个月至少读过1条假新闻,而至少50%的民众表示相信他们当时读过的假新闻。最重要的是,社交媒体并没有将所有新闻公平地呈现给大众,因为个性化功能导致普通人只读他们想读的新闻,结果导致大多数人读到的新闻高度倾向他们喜欢的总统候选人。这些原因导致假新闻对2016年的总统选举造成了决定性影响[10]。

虽然假新闻对这次美国选举影响巨大,但是这些假新闻的最大来源并非来自美国。《Wired》调查发现,2016年总统选举期间,网络假新闻的最大炮制者来源于东欧国家马其顿[11]。马其顿的一个只有5万人的小镇成为100多个支持川普网站的注册地。这些网站刊登了大量支持川普的假新闻,包括希拉里·克林顿即将被起诉以及教皇支持唐纳德·特朗普等。这些假新闻网站的操纵者将新闻链接大量发布到Facebook、Twitter等社交媒体上,吸引唐纳德·特朗普支持者点击和分享,给这些网站带来大量流量。与此同时,操纵者在这些网站上通过谷歌广告平台安插了大量广告,为其带来了可观的点击收入。

假新闻其实早已影响到世界各国,这次被曝光是因为影响到了美国总统大选。对此美国国会已经在2017年进行了几次听证会,调查Facebook、谷歌、Twitter等社交媒体在整个过程中扮演的角色,并责成这些公司采取技术手段尽量消除假新闻及其带来的影响。

7　虚拟币泡沫化与勒索病毒的威胁

区块链技术驱动的比特币在从2017年初的每枚1000美元上涨到2017年12月份的接近2万美元,成为科技金融领域本年度最大关注热点。

中本聪在2008年悄悄注册了比特币网站,通过一篇论文和自己编写的比特币软件和区块链技术以开源软件方式引入互联网[12]。2009年1月,中本聪创建了比特币的第1个区块,挖掘了50个比特币,后来陆续挖掘了1100万枚左右比特币。在随后2年时间里,比特币只是在虚拟货币群这个小圈子里为大家研究和讨论,并没有传播到整个互联网。一直到2010年,比特币才被一些圈外的商家接受,其中包括2010年5月份世界上的第1笔比特币购物交易:一个程序员用1万枚比特币购买了2个棒约翰比萨饼。

比特币在2011年首次达到与美元1∶1兑换后,在2013年一度升值到每枚1242美元,但随后2015年跌至不足200美元。2016年人民币贬值导致比特币再次升值,升至700多美元。2017年伊始,比特币继续升值到1000美元以上,尽管中国在9月份禁止了比特币交易,但是美国、日本和韩国将引入比特币期货交易的传闻不断推升起上涨趋势。2017年12月中旬,每枚比特币一度达到2万美元,其上升规模和时间比例仅次于17世纪荷兰郁金香泡沫,成为近500年来世界上最大的金融资产泡沫。

比特币在2017年的泡沫式增长也导致其他虚拟加密货币的发展。其中以太币(Ethereum)和莱特币(Litecoin)分别从2017年初的9美元和4美元上涨到900美元和322美元左右,从泡沫程度来看远超比特币。这些虚拟加密货币从技术角度来看与比特币没有本质区别,只是略加改进,但因为从众较少,所以目前没有比特币的影响力大[13]。

比特币目前主要还是暗网的支付手段。虚拟加密货币是否可以在未来真正成为主流支付工具还是未知数。区块链技术的核心是每一笔交易需要并入一个区块,然后该区块包含的交易得到所有网络内服务器的承认和记录。当交易量以几何级数增加时,区块大小的选择成为关键,如果区块比较大,每次处理的交易比较多,效率就比较高,但是需要更长的时间才能被网络内所有服务器认可,造成用户长时间等待;如果缩小区块链,会提高交易处理速度,减少用户等待时间,但是会导致服务器之间处理不一致而产生冲突。这种模式是否能够支撑不断增加的交易需求将是比特币面临的实际问题,对此已经有不少专家提出了改进方案[14]。

2017年另一个与比特币高度相关的热点是勒索软件(ransomware)的横行。在此之前,僵尸网络已经成为互联网上最主要的黑客入侵和控制普通用户计算机的手段。不过早期的僵尸网络都是黑客在计算机后端控制,用户对此没有察觉。黑客往往利用用户计算机滥发垃圾邮件、挖矿,或者对其他目标进行拒绝服务攻击(DoS attack)。勒索则是这一控制形式的升级。黑客在控制了用户计算机后,将用户计算机硬盘加密,然后勒索用户用比特币作为赎金来为硬盘数据解密[15]。

2017年5月,WannaCry比特币勒索病毒事件就是这类方式。这一病毒攻击涉及到包括中国大学校园学生计算机在内的全球99个国家近10万台电脑,造成不同程度的用户数据丢失。值得一提的是,在2017年4月14日网络黑客影子掮客在网上公布了美国国家安全局开发的计算机操作系统漏洞利用程序,其中包括用来攻击微软视窗操作系统的"永恒之蓝"(Eternal-Blue)。业内人士透露WannaCry病毒是受"永恒之蓝"启发改编而成。尽管修复该漏洞的安全补丁已经在2017年3月14日发布,很多计算机并没有及时更新,尤其是较早的视窗系统和因安装了盗版视窗操作系统而无法升级的计算机(图8)。

图8 Wana Decrypt0r 2.0程序截图

8 结论与展望

2017年的信息科学领域继续呈现飞速发展的势头。各行各业对人工智能的应用需求和加强学习算法的成功使得这一领域在未来几年有了更明确的研究发展方向。人工智能和物联网技术所推动的智能家庭的不断普及将为人们的生活带来更多的便利和效率。机器人仿真技术的发展和完善则不但对制造业,也对服务行业和军事领域产生巨大冲击。服务行业更多的就业机会将会被具有自然语言对话能力的机器人所占据;未来的军事冲突将会有越来越多的机器人参与,当一个国家的军事力量的绝大部分是由机器人构成时,其政治生态也会受到影响。

人工智能所带来的各种社会问题在2017年也不断出现,例如通过分析和处理大数据产生的各种预测和选择模型不可避免地掺杂着人类的看法和偏见,人工智能技术支撑的社交媒体在给用户提供了充分个性化的新闻组合的同时,滋生了假新闻的泛滥。诸如勒索病毒等信息安全问题继续对人们构成威胁,必须解决好这些新的挑战才能更好地享受信息科技发展带来的福利。

量子计算机在2017年有了重要的突破,具备50个量子比特的计算机将可以超过目前世界上最快的超级计算机的运算能力,从而掌握量子霸权,这一即将实现的前景对信息科学的很多领域(包括人工智能和加密技术)都会产生巨大影响,如何面对这一现实应该现在就成为各个领域从业者思考的问题。

参考文献(Reference)

[1] Silver D, Schrittwieser J, Simonyan K, et al. Mastering the game of Go without human knowledge[J]. Nature, 2017, 550 (7676): 354-359.

[2] Silver D, Hubert T, Schrittwieser J, et al. Mastering chess and shogi by self-play with a general reinforcement learning algorithm[J]. 2017, arXiv: 1712.01815.

[3] Preskill J. Quantum computing and the entanglement frontier[J/OL]. [2017-12-20]. http://www.theory.caltech.edu/~preskill/talks/Simons-2013-preskill.pdf.

[4] Yin J, Cao Y, Li Y H, et al. Satellite-based entanglement distribution over 1200 kilometers[J]. Science, 2017, 356(6343): 1140-1144.

[5] Apthorpe N, Reisman D, Feamster N. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic[EB/OL]. [2017-12-20]. http://www.internetsociety.org/sites/default/files/Poster-SmartHomeNoCastle%20(2).pdf.

[6] Nobili S, Scona R, Caravagna M, et al. Overlap-based ICP tuning for robust localization of a humanoid robot[C]//IEEE International Conference on Robotics and Automation. Piscataway, NJ: IEEE, 2017: 4721-4728.

[7] Neff G, Nagy P. ATalking to bots: Symbiotic agency and the case of tay[J/OL]. [2017-12-20]. http://ijoc.org/index.php/ijoc/article/download/6277/1804.

[8] Hankerson D, Marshall A R, Booker J, et al. Does technology have race?[C]//Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. New

York: ACM, 2016: 473-486.
[9] Caliskan A, Bryson J J, Narayanan A. Semantics derived automatically from language corpora contain human-like biases[J]. Science, 2017, 356(6334): 183-186.
[10] Allcott H, Gentzkow M. Social media and fake news in the 2016 election[J]. Journal of Economic Perspectives, 2017, 32 (2): 211-236.
[11] Subramanian S. Inside the macedonian fake-news complex[J/OL]. Wired Magazine, [2017-12-20]. https://www.wired.com/2017/02/veles-macedonia-fake-news/.
[12] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J/OL]. [2017-12-20]. http://nakamotoinstitute.org/bitcoin/.
[13] Extance A. The future of cryptocurrencies: Bitcoin and beyond [J]. Nature, 2015, 526(7571): 21-23.
[14] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-NG: A scalable blockchain protocol[C/OL]. [2017-12-20]. http://www.usenix.org/sites/default/files/conference/protected-files/nsdi16_slides_eyal.pdf.
[15] Adamov A, Carlsson A. The state of ransomware. Trends and mitigation techniques[C]//2017 IEEE East-West Design & Test Symposium (EWDTS). Piscataway, NJ: IEEE, 2017: 1-8.

Summary of hot research topics in information technology in 2017

WAN Yun

University of Houston-Victoria, Texas 77901, USA

Abstract This article samples the hot research topics in information technology in 2017. We review the reinforcement learning that showed great promise in AI application, the quantum computer research which reached a 50 qubit competition stage, smart home that is increasingly popular among general public, and more mature robot simulation technology. Meanwhile, we also experienced major challenges in 2017. For example, AI algorithms were found to be biased due to existing data containing human bias; researchers found fake news had major impact on 2016 U.S. Presidential election; bitcoin value increased dramatically and was more like a bubble; ransomware threatening computer users was getting worse.

Keywords artificial intelligence; quantum computer; bitcoin; ransomware

（责任编辑　刘志远）